

FEB 20 2007

Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006**REMARKS**

In the present Office Action, the Examiner rejected claims 1-40. Claims 2, 7, 8, 12, 20, 21 and 28 remain canceled. Claims 1 and 13 are amended. Additionally, the specification is amended. No new matter has been added. As such, claims 1, 3-6, 9-11, 13-19, 22-27, and 29-40 are pending. In view of the following remarks, Applicants respectfully request reconsideration and allowance of all pending claims.

**Rejections Under 35 U.S.C. § 101**

In the Office Action, the Examiner rejected claims 1, 3-6, 9-11, 13-19, 22-27 and 29-35 under 35 U.S.C. § 101 for failing to produce a tangible result. *See* Office Action, page 7. Specifically, the Examiner asserted that the claimed invention fails to meet the statutory requirements for patentability under 35 U.S.C. § 101 because the claims recite “nonfunctional descriptive material stored in a computer-readable medium” and fail to produce “useful, concrete and tangible” results to have a practical application. *See id* at pages 3-4. Applicants respectfully traverse this rejection.

The Supreme Court has observed that Congress intended Section 101 to include “anything under the sun that is made by man.” *Diamond v. Chakrabarty*, 447 U.S. 303, 308-9, 206 U.S.P.Q. 193, 197 (1980). There are, however, qualifications to the apparent sweep of this statement. Excluded from patentability are subject matter in the categories of “laws of nature, natural phenomena and abstract ideas.” *Diamond v. Diehr*, 450 U.S. 175, 185, 209 U.S.P.Q. 1, 7 (1981). However, other than these specific exceptions, nearly anything man made is statutorily patentable subject matter under Section 101.

Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

The Federal Circuit has developed a test which may be used to determine if a claim recites statutory subject matter, namely does the claim produce a “*useful, concrete, and tangible result.*” *In re Alappat*, 31 U.S.P.Q.2d 1545, 1557 (Fed. Cir. 1994) (*en banc*) (emphasis added). The Federal Circuit elaborated on this test by holding that one must look to “the essential characteristics of the subject matter, in particular, its *practical utility.*” *State Street Bank & Trust Co. v. Signature Fin. Group Inc.*, 47 U.S.P.Q.2d 1596, 1602 (Fed. Cir. 1998) (emphasis added). Further, in explaining the “useful, concrete, and tangible” test, the Federal Circuit has stated “the dispositive inquiry is whether the claim *as a whole* is directed to statutory subject matter.” *In re Alappat*, 31 U.S.P.Q.2d at 1557 (Fed. Cir. 1994) (emphasis added). Indeed, there has been no requirement from Congress, the Supreme Court, or the Federal Circuit mandating that a *specific final result* be shown for a claim to qualify under 35 U.S.C. § 101. *See id.* Rather, the Federal Circuit has specifically stated “the *Alappat* inquiry simply requires an examination of the contested claims to see if the claimed subject matter *as a whole* is a disembodied mathematical concept representing nothing more than a ‘law of nature’ or an ‘abstract idea,’ or if the mathematical concept has been reduced to *some practical application rendering it ‘useful.’*” *AT&T Corp. v. Excel Communications, Inc.*, 50 U.S.P.Q.2d 1447, 1451 (Fed. Cir. 1999) (emphasis added). Therefore, if a claim, read as a whole and in light of the specification, produces any useful, concrete, and tangible result, the claim meets the statutory requirements of 35 U.S.C. § 101. *See id.*

In rejecting the present claims under 35 U.S.C. § 101, the Examiner relied heavily on *Arrhythmia Research Tech., Inc. v. Corazonix Corp.*, 22 U.S.P.Q.2d 1033 (Fed. Cir. 1992). The patent at issue before the Federal Circuit in *Arrhythmia* claimed a method for analyzing electrocardiograph signals to determine the presence or absence of a predetermined level of

Serial No. 09/966,890.  
Amendment and Response to  
Office Action Mailed November 29, 2006

high-frequency energy in the late QRS signal. *See id.* at 1038. However, the court ultimately held that while the final output of the claimed process was a numerical result, such did not preclude patentability because the number was “not a mathematical abstraction; it [was] a measure in microvolts of a specified heart activity.” *Id.* The court also embraced the view that *the tangibility requirement does not preclude electrical signals. See id.*

The Federal Circuit has further explored issues regarding manipulation of data in the form of electrical signals. In *State Street Bank & Trust Co. v. Signature Fin. Group, Inc.*, 149 F.3d 1368, 47 U.S.P.Q.2d 1596, 1601 (Fed. Cir. 1998), *cert denied*, 525 U.S. 1093 (1999), the patent at issue claimed a process for administrating and accounting mutual funds. The Federal Circuit held that the “transformation of data, representing discrete dollar amounts, by a machine through a series of mathematical calculations into a final share price, constitutes a practical application of a mathematical algorithm, formula, or calculation, because it produces a *useful, concrete, and tangible result* – a final share price momentarily fixed for recording and reporting purposes.” *Id.* (emphasis added).

Applicants respectfully assert that independent claims 1, 13, 19 and 27, taken as a whole, each recite statutory subject matter under 35 U.S.C. § 101 because they produce a useful, concrete and tangible result. The present application is directed to generating a random number for use in generating a cryptographic key in a cryptographic security system. Specifically, the present application discloses methods and apparatus for enabling a cryptographic security algorithm and initializing and restoring security data used to generate pseudo-random keys for the cryptographic security algorithm. *See* Specification, page 13, lines 18-22; page 23, lines 4-15. The result of the initialization or restoration of security data

Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

is a fully populated or randomized seed pool, which may be indicated by a state bit, or alteration of a signature value stored in the seed pool, and from which a cryptographic key may be generated. *See id.* at page 17, lines 7-22; page 24 line 6 to page 25, line 10.

***Independent claims 1 and 13***

Independent claim 1, as amended, recites, *inter alia*, “[a] method of *generating a cryptographic key* for a cryptographic security subsystem of a processor-based device, the method comprising the acts of...writing one or more bits of data to a seed pool...examining the state bit to determine whether the seed pool is full...and [if full], *generating a pseudo-random number* from the seed pool, *wherein the pseudo-random number is used to generate the cryptographic key* for the cryptographic security subsystem.” (Emphasis added).

Independent claim 13, as amended, recites, *inter alia*, “[a] method of initializing a seed pool for generating a cryptographic key for a cryptographic security subsystem of a processor-based device, the method comprising the acts of...writing one or more bits of data to the seed pool...enabling the cryptographic subsystem when more than a predetermined portion of the signature value of the seed pool has been altered...and *generating a pseudo-random number* from the seed pool, *wherein the pseudo-random number is used to generate the cryptographic key* for the cryptographic security subsystem.” (Emphasis added).

Applicants respectfully assert that generating a pseudo-random number, wherein the pseudo-random number is used to generate a cryptographic key, as recited in independent claims 1 and 13, clearly yields a useful and tangible result. *See Arrhythmia Research Tech. Inc., v. Corazonix Corp.*, 22 U.S.P.Q.2d 1033, 1039 (Fed. Cir. 1992) (holding that physical tangibility goes so far as to encompass electrical signals). Furthermore, contrary to the

Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

Examiner's position, Applicants assert that the claimed subject matter generates concrete and useful results because, although the resulting seed pool and cryptographic keys are numerical in nature, they constitute more than mere mathematical abstractions. As a whole, the claims are directed to a practical application (populating a seed pool and generating a cryptographic key) as opposed to a disembodied mathematical concept. Specifically, the populated seed pool is the result of masking into the seed pool a series of random bits based on triggering events to ensure a high degree of randomness. The resulting seed pool is then used to generate cryptographic keys with a similarly high degree of randomness. The purpose of ensuring a high degree of randomness is for increased security and integrity in computing systems. Computer security is becoming increasingly important in today's environment of heavily networked computer systems. As a result, security and integrity features are becoming increasingly desirable in the use of personal computers and servers. Such cryptographic keys may be useful in permitting secured communications between different computers and servers, as well as preventing unauthorized access from rogue or external devices. *See* Specification, page 2, lines 20-25 to page 3, lines 1-4.

Accordingly, the claimed methods recited in independent claims 1 or 13 produce useful, concrete, and tangible results and, therefore, Applicants respectfully request withdrawal of the rejection under 35 U.S.C. § 101 of independent claims 1 and 13, as well as all claims depending therefrom.

***Independent claims 19 and 27***

As discussed previously, the Federal Circuit has held that a claim is statutorily patentable subject matter if the claim produces a "*useful, concrete, and tangible result.*" *In re*

Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

*Alappat*, 31 U.S.P.Q.2d 1545, 1557 (Fed. Cir. 1994). The patent at issue in *Alappat* claimed a machine for creating a smooth waveform in a digital oscilloscope through a series of anti-aliasing calculations. *See id.* at 1555. On review, the Federal Circuit reached the conclusion that although the elements recited in the claims represent circuitry elements that perform mathematical calculations, “the claimed invention *as a whole* is directed to a combination of interrelated elements which combine to form a machine for converting discrete waveform data samples into anti-aliased pixel illumination intensity data.” *Id.* at 1557 (emphasis added). Ultimately, the *Alappat* court held that the claimed device was not a disembodied mathematical concept, “but rather a specific machine to produce a useful, concrete, and tangible result.” *Id.*

Applicants respectfully assert that independent claims 19 and 27 are clearly directed to statutorily patentable subject matter under Section 101. Independent claim 19 recites, *inter alia*, “[a] processor-based device comprising...a memory system...a communications management system...wherein the communications management system comprises...security logic...wherein the security logic is configured to...examine the state bit to determine whether the seed pool is fully populated; write one or more bits of data to the seed pool.” (Emphasis added). Independent claim 27 recites, *inter alia*, “[a] processor-based device comprising...a memory system...a communications management system...wherein the communications management system comprises...security logic...wherein the security logic is configured to... write one or more bits of data to the seed pool, the bits altering a signature value; determine whether the plurality of data bits in the seed pool has at least a portion of the signature value.” (Emphasis added).

Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

Like the claimed device in *Alappat*, independent claims 19 and 27 are directed to a combination of interrelated hardware elements, such as a communication system comprising an interface controller, a non-volatile memory device, and security logic, all of which combine to form a machine for achieving a useful and tangible result. Specifically, independent claim 19 is directed to a device for generating a cryptographic key from a seed pool, and independent claim 27 is directed to a device for enabling or disabling a cryptographic security algorithm. As previously discussed, the use of pseudo-random cryptographic keys is a useful, concrete, and tangible result for maintaining security and integrity in personal computers and servers. Accordingly, Applicants respectfully request withdrawal of the rejection under 35 U.S.C. § 101 of independent claims 19 and 27, as well as all claims depending therefrom.

#### **Rejections Under 35 U.S.C. § 103(a)**

In the Office Action, the Examiner rejected claims 1, 3-6, 9-11, 13-19, 22-27, and 29-35 under 35 U.S.C. § 103(a) as being unpatentable over Bruce Schneier's "Applied Cryptography," (hereinafter referred to as "the Schneier reference") and further in view of Utz et al., U.S. Patent No. 5,680,131 (hereinafter referred to as "the Utz reference"). Applicants respectfully traverse this rejection.

#### ***Legal Precedent***

The burden of establishing a *prima facie* case of obviousness falls on the Examiner. *Ex parte Wolters and Kuypers*, 214 U.S.P.Q. 735 (PTO Bd. App. 1979). To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 180 U.S.P.Q. 580 (CCPA 1974). The mere fact that

Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

references *can* be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 16 U.S.P.Q.2d. 1430 (Fed. Cir. 1990). Accordingly, to establish a *prima facie* case, the Examiner must not only show that the combination includes *all* of the claimed elements, but also a convincing line of reason as to why one of ordinary skill in the art would have found the claimed invention to have been obvious in light of the teachings of the references. *Ex parte Clapp*, 227 U.S.P.Q. 972 (B.P.A.I. 1985).

***Independent claims 1, 19 and 36: Neither the Schneier nor the Utz reference teaches or discloses determining if a seed pool is full***

Independent claim 1, as amended, recites, *inter alia*, "writing one or more bits of data to a seed pool upon termination of the first type of triggering event, the seed pool comprising a *state bit* indicative of a state of the seed pool... masking one or more bits of data to the seed pool upon termination of the second type of triggering event... examining the state bit to *determine whether the seed pool is full.*" (Emphasis added). Independent claim 19 recites, *inter alia*, "a non-volatile memory device to store a seed pool, wherein the seed pool comprises a *state bit* indicative of the state of the seed pool...security logic...wherein the security logic is configured to...*examine the state bit to determine whether the seed pool is fully populated.*...and mask one or more bits of data to the seed pool upon termination of the second type of triggering event." (Emphasis added). Independent claim 36 recites, *inter alia*, "[a] method for restoring security data to non-volatile memory in a computer comprising... *tracking the state of the seed pool to determine if the seed pool is fully populated.*" (Emphasis added).



Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

In rejecting independent claims 1, 19 and 36, the Examiner asserted that page 428, lines 16-18 of the Schneier reference discloses "examining [a] state bit to determine whether the seed pool is full." *See* Office Action, page 8. However, a careful analysis of the cited passage does not appear to reveal such a teaching. The cited passage addresses the problem of having to repopulate a seed pool in the absence of triggering events between system reboots. Rather than suggesting a method for solving this problem, the author states "there is *no solution to this problem other than to wait* until enough external random events have taken place." *See* Schneier, page 428, lines 16-18 (emphasis added). Applicants believe the cited passage is absent of any language teaching or suggesting determining when a seed pool is full by use of a state bit, or by any other method. Indeed, the Examiner seems to concede with Applicants' position by later asserting "Schneier fails to *specifically* mention determining if a seed pool is full." *See* Office Action, page 9 (emphasis in original).

Nevertheless, the Examiner goes on to assert that the Utz reference obviates the deficiencies of the Schneier reference. Specifically, the Examiner stated "Utz discloses... determining if the seed pool is full...and writing one or more bits of data to the seed pool upon termination of the second type of triggering event if the seed pool is not full (UTZ col. 3 lines 38-40; col. 11 lines 51-55)." *See id.* (emphasis added). However, after careful review, the cited passages do not appear to reveal such teaching. Instead, the cited passages in the Utz reference describe the use of a pseudo-random number generator to generate a randomized synchronization code which is transmitted to a receiving unit. *See* Utz, col. 3, lines 20-22. Verification codes are then generated by incrementing the pseudo-random number generator. *See id.* at col. 3, lines 38-40. Also discussed are possible variable features

Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

of the transmitting unit, including the possibility of generating different synchronization codes after successive applications of power. *See id.* at col. 11, lines 51-55.

However, it does not appear that the Utz reference *ever* addresses a situation in which the non-volatile memory encounters a scenario in which the fixed start values (seed pool) are lost, nor does it describe using a state bit or any other method to determine when these values are repopulated into the non-volatile memory. Indeed, the Utz reference appears to be absent of any language teaching or suggesting *determining whether a seed pool is full* by use of a *state bit*, as set forth in the independent claims 1, 19 and 36, or by any other method.

In the most recent Office Action, the Examiner further asserted that column 7, lines 21-25 and 60-62, and column 8, lines 5-9, of the Utz reference discloses a state indicator for determining if a seed pool is full. *See* Office Action, page 6. Applicants thank the Examiner for providing the additional passages, however, a careful analysis of the additional cited passages does not appear to reveal such teaching. The cited passages teach that when the push button is depressed, the transmitting unit generates a new code (through the shifting and multiplexing of fixed start values loaded into the 11-bit, 13-bit, and 16-bit RS/PRNG circuits from the non-volatile memory) and transmits it to the receiving unit for verification. *See* Utz, col. 7, lines 19-25 and lines 58-65. Contrary to the Examiner's position that the push button acts as a state indicator for determining when a seed pool is full, the push button described in the Utz reference merely determines when a matching verification code is found or when a predetermined number of reference codes have been generated. *See id.* at col. 8, lines 1-14. Thus, it does not appear that the additional cited passages teach or suggest determining when a seed pool is full by examining a state bit, or by any other method.

Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

For at least this reason, the Utz reference fails to obviate the deficiencies of the Schneier reference with regards to independent claims 1, 19 and 36. Accordingly, the Schneier and Utz references, taken alone or in hypothetical combination, cannot support a *prima facie* case of obviousness under 35 U.S.C. § 103. Applicants respectfully request withdrawal of the rejection of independent claims 1, 19 and 36, as well as all claims depending therefrom.

***Independent claims 13 and 27: The Utz reference does not teach or disclose the altering of a signature value***

Independent claim 13, as amended, recites, *inter alia*, “[a] method of initializing a seed pool...comprising the acts of: (a) prior to enabling the cryptographic security subsystem, writing a plurality of bits of data to a seed pool, the plurality of bits having a signature value...(c) writing one or more bits to the seed pool upon termination of the first type of triggering event, the one or more bits of data *altering the signature value of the seed pool*... (d) enabling the cryptographic security subsystem when more than a predetermined portion of the signature value of the seed pool has been altered.” (Emphasis added).

Independent claim 27 recites, *inter alia*, “A processor-based device comprising...a non-volatile memory device to store a seed pool comprising a plurality of data bits; and security logic in communication with ... the non-volatile memory device....wherein the security logic is configured to: write the one or more bits to the seed pool, the bits *altering a signature value*; determine whether a plurality of data bits in the seed pool has at least a portion of the signature value; and disable establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value.” (Emphasis added).

Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

In sharp contrast, the Utz reference does not appear to teach or suggest altering a signature value to determine when to enable a cryptographic security subsystem, as recited in independent claims 13 and 27. In rejecting claims 13 and 27, the Examiner correlated the "start value" of the Utz reference with the "signature value" of the present claims. *See* Office Action, page 10. The "start value" of the Utz reference, however, is never altered because it is used as an identifying value for a receiver to recognize a remote transmitting device. *See* Utz, col. 6, line 65 to col. 7, line 18. The "start value" is programmed to be specific to the particular transmitting unit, although several bits may be common to multiple transmitting units. *See id.* at col. 6, lines 30-35. To preclude alteration of the "start value," a disable fuse makes the nonvolatile memory where the "start value" is stored *one-time* programmable; thus, the start value is *fixed*. *See id.* col. 8, line 58 to col. 9, line 4.

The "start values" are used in the generation of a "synchronization code." The transmitting unit of the Utz reference has an 11 bit RS/PRNG, a 13 bit RS/PRNG and a 16 bit RS/PRNG. *See* Utz, col. 6, lines 37-61. The 11 bit RS/PRNG and 13 bit RS/PRNG are loaded with a "start value" from a non-volatile memory. *See id.* at col. 5, lines 34-42. When a pushbutton is depressed, the "start values" from the 11 bit RS/PRNG and the 13 bit RS/PRNG are serially supplied to a transmitter circuit. *See id.* at col. 6, lines 37-61. Additionally, the 16 bit RS/PRNG generates a pseudo-random number which is serially supplied to the transmitting circuit. *See id.* The transmitting circuit then transmits a serial bit stream which includes the "start values" from the 11 and 13 bit RS/PRNG and the pseudo-random number from the 16 bit RS/PRNG. *See id.* The serially-combined bit stream is called the "synchronization code." *See id.* Throughout this process, however, the "start

Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

values" are never altered. Indeed, as mentioned above, they are intended to remain *unaltered* so they can be used as an identifier for the transmitting unit.

In the most recent Office Action, the Examiner further asserted that column 8, lines 31-43 of the Utz reference discloses altering a signature value. *See* Office Action, page 6. Applicants thank the Examiner for providing the additional passage, however, a careful analysis of the cited passage does not appear to reveal such teaching. The cited passage teaches that a transmitting unit generates different successive codes in order to prevent intruders from stealing the code with a code copier, or some similar device. *See* Utz, col. 8, lines 14-41. Contrary to the Examiner's position, the generation of differing codes is not the altering of a signature value, as they are derived from constant fixed start values stored in non-volatile memory. *See id.* at col. 5, lines 34-42. It does not appear the cited passage teaches or suggests altering the fixed start values. As discussed above, the start values are *not intended to be altered* because they are used as an identifying value for a receiver to recognize a corresponding remote transmitting device. *See id.* at col. 6, line 65 to col. 7, line 18. Consequently, the cited passage fails to teach the altering of a signature value in a seed pool to enable a cryptographic security subsystem, as recited in independent claims 13 and 27.

Accordingly, the Utz and Schneier references, taken alone or in hypothetical combination, fail to disclose all the elements of claims 13 and 27. As such, a *prima facie* case for obviousness under 35 U.S.C. § 103 has not been presented. Therefore, Applicants respectfully request withdrawal of the rejection of claims 13 and 27, as well as all claims depending therefrom.

FEB 20 2007

Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

In view of the foregoing discussion, Applicants respectfully request withdrawal of the 35 U.S.C. § 103 rejection and further request allowance of independent claims 1, 13, 19, 27 and 36, as well as all claims depending therefrom.

**Conclusion**

Applicants respectfully submit that all pending claims should be in condition for allowance. However, if the Examiner wishes to resolve any other issues by way of a telephone conference, the Examiner is kindly invited to contact the undersigned attorney at the telephone number indicated below.

FEB 20 2007


Serial No. 09/966,890  
Amendment and Response to  
Office Action Mailed November 29, 2006

**General Authorization for Extensions of Time**

In accordance with 37 C.F.R. § 1.136, Applicants hereby provide a general authorization to treat this and any future reply requiring an extension of time as incorporating a request therefor. Furthermore, pursuant to 37 C.F.R. § 1.17(e), Applicants authorize the Commissioner to charge the appropriate Request for Continued Examination fee of \$790.00 to Deposit Account No. 08-2025; Order No. COMP:0224/FLE/PET. Further, the Commissioner is authorized to charge any fees that may be due at this time or at time during the pendency of this application to the Deposit Account listed.

Respectfully submitted,

Date: February 20, 2007

  
\_\_\_\_\_  
Michael G. Fletcher  
Reg. No. 32,777  
FLETCHER YODER  
(281) 970-4545

**Correspondence Address:**

IP Administration  
Legal Department, M/S 35  
HEWLETT-PACKARD COMPANY  
P.O. Box 272400  
Fort Collins, CO 80527-2400